Title:

PRIVATE PROPERTY PROTECTION IN PUBLIC SYSTEMS USING SMART CARD

Inventor:
Robert R. Silverman
US Citizen

655 S. Fairoaks, M313
Sunnyvale, CA 94086
(415) 235 5374

rrsilver@telocity.com

Created December 1, 2001

Application Information	Application Type	regular
	Subject Matter	utility
	Suggested classification	Computer science
	Title	Private Property Protection in Public Systems Using Smart Card
	Small entity	yes
	Petition included	no
Applicant Information	Applicant authority type	inventor
	Primary Citizenship	US
	Status	Full capacity
	Given name	Robert
	Middle name	Roosevelt
	Family name	Silverman
	Street	655 S. Fairoaks Ave, M313
	City of residence	Sunnyvale
	Sate	CA
	ZIP	94086
	email	rrsilver@telocity.com
Correspondence Information	Same as applicant	
Representative Information	Same as applicant	

Table of Contents

RELATED APPLICATIONS 3

FIELD OF INVENTION 3

PRIOR ART 3

LIST OFADDITIONAL MATERIALS 3

TERMINOLOGY 4

THE PROBLEM 5

OVERVIEW OF THE INVENTION 5

DETAIL DESCRIPTION OF THE INVENTION 6

SOLUTION 1 ..... *6*
Systems comprising Solution 1: 6
Operation of Solution 1 6

SOLUTION 2 ..... *7*
Systems comprising Solution 2: 7
Operation of Solution 2 7

SOLUTION 3 ..... *8*
Systems comprising Solution 3: 8
Operation of Solution 3 8

CLAIMS 9

Claim 1: *9*

Claim 2: *9*

Claim 3: *9*

Claim 4: *9*

ABSTRACT 10

RELATED APPLICATIONS

None.

FIELD OF INVENTION

The field of invention is an application of Smart Card technology to locking publicly accessible machines.

Keywords: Smart Card, session key, security, cryptography.

PRIOR ART

The following technologies already exist individually and we have no invention claims on them.
We have no invention claims on: Smart Card with Memory only, Smart Card with CPU (microprocessor), Card Acceptance Device (CAD), major appliances such as washer, dryer, microwave oven, electronically controlled door, and random number generator.

I have not found any application of Smart Card technology to this type of problem searching on US PTO and on Delphion.com.

LIST OFADDITIONAL MATERIALS

None.

TERMINOLOGY

term	**description**
SC	Smart Card. Two types of SC described below.
MSC	Memory Smart Card Device. Smart Card, which has persistent memory but no CPU.
CSC	CPU (Microprocessor) Smart Card Device. Smart Card, which contains microprocessor and persistent memory.
IM	Instrumented machine. A machine instrumented with the locking mechanism which details are discussed below. We will present multiple solutions to the problem.
Session	A set of related operations. In our case, a session is delimited by two operations: locking the instrumented machine at the start, and subsequent unlocking of the machine at the end.
SK	Session key. A string of bytes, which is randomly generated and is unique for this session.
SKSC	Session Key stored in Smart Card.
SKIM	Session Key stored in the instrumented machine.
LDC	Logic Decision Circuit. Logic circuit included in the instrumented machine.
MBS	Microprocessor Based System. Microprocessor Based System included in the instrumented machine. It is an alternate (programmable) implementation of LDC.
CAD	Card Acceptance Device. Equipment used to read and write smart cards.
ECD	Electrically controlled door. Machine door that can be locked and unlocked under the control of the Logic Decision Circuit.

THE PROBLEM

In this proposal we are solving the following problem. Consider a public machine that operates in a time-shared fashion on a private property. An example of such machine is a Laundromat or a laundry room in a building shared by the tenants in an apartment complex.

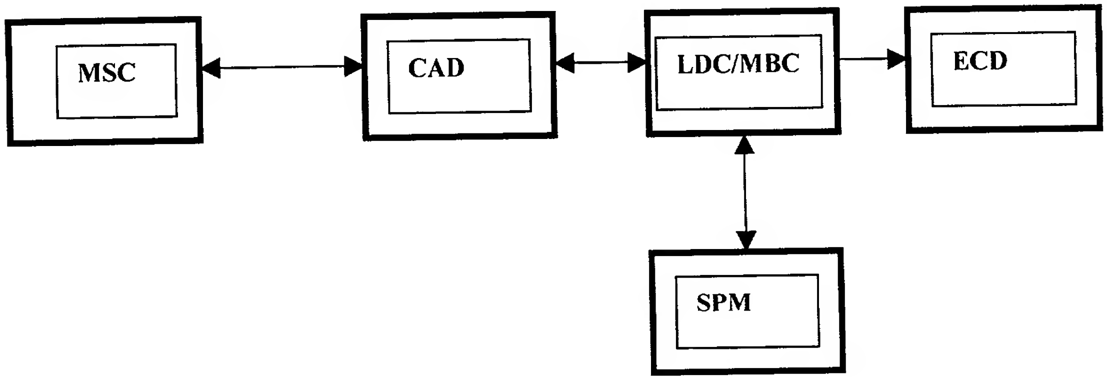
In this case the specific problem is this. We would like to protect the private property such as one person's clothing while it is being operated on by the instrumented machine (for example clothes are being washed) in a publicly accessible location.

OVERVIEW OF THE INVENTION

Using the example of Laundromat as a domain of problem, the invention operates as follows. The user is equipped with a Smart Card (MSC). The washing machine is instrumented with the following subsystems, a (1) Card Acceptance Device (CAD), (2) a Logic Decision Circuit (LDC), (3) a Small Persistent Memory (SPM), and (4) an electrically controlled door (ECD). See figure below.

The LDC contains a hardware or software program to generate a session key (SK). The MSC will store the SK in its memory (as SKSC). Similarly, the LDC will store the SK (as SKIM) in its memory (SPM) and lock the door. Note that the SKSC is session key stored in MSC. Note that the SKIM is the same session key stored in the SPM of the instrumented machine.

Upon reinserting of the same MSC into the CAD, the LDC reads the SKSC from the MSC and compares the SKSC with its own SKIM from SPM. If there is match, the logic will open the door lock. Because the SK is very long string of bytes, it is hard to forge.
This method guarantees that only the original person who inserted the clothes into the washer will be able to retrieve his clothes.



DETAIL DESCRIPTION OF THE INVENTION

We will describe different solutions to the problem under discussion.

SOLUTION 1

In this section we will describe the subsystems comprising the Solution 1.

Systems comprising Solution 1:

The total system consists of two subsystems.
(1) Memory Smart Card (MSC) (carried by the user), contains memory only, no CPU.
(2) System attached to the instrumented machine (for example a washer or dryer).

The instrumented machine system consists of the following subsystems.
(2.1) Card Acceptance Device (CAD).
(2.2) A Logical Decision Circuit (LDC). Capabilities: generation of session key, comparison of two keys, lock door, unlock door.
(2.3) Small Persistent Memory (SPM).
(2.4) Electronically Controlled Door (ECD).

Operation of Solution 1

In this section we will describe the operation of the Solution 1 using pseudocode.

High-level operation of the system during start stage.

```
User selects an unused instrumented machine.
User loads the machine with his/her clothing for normal operation.
User inserts MSC into the instrumented machine CAD.
The LDC computes a session key (SKIM).
The LDC stores the SKIM in its persistent memory.
The LDC stores a copy of the session key SKSC in the smart card persistent memory.
(Note that the value of SKIM is identical to SKSC, but they are stored in different places.)
The LDC locks the door of the instrumented machine.
The user pushes proper start buttons of the instrumented machine.
The instrumented machine starts its normal operation.
(At this point, the user is free to leave the instrumented machine, since the door is safely locked.)
```

High-level operation of the system during stop stage.

```
The user returns to the instrumented machine.
The user inserts the MSC into the instrumented machine CAD.
The LDC reads the session key SKSC from the smart card.
The LDC reads its session key SKIM from its persistent memory.
The LDC compares the SKSC and SKIM for equality.
If the compare operation results in an equality, the LDC issues command to unlock the door.
The user removes the smart card from the CAD.
The user removes his/her possessions from the instrumented machine.
If the compare results in inequality, the door will remain locked.
```

SOLUTION 2

In this section we will describe the subsystems comprising the Solution 2.

Systems comprising Solution 2:

The total system consists of two subsystems.

1. Memory Smart Card (MSC) (carried by the user), contains memory only, no CPU.
2. System attached to the instrumented machine (for example a washer or dryer).

The instrumented machine system consists of the following subsystems.
(2.1) Card Acceptance Device (CAD).
(2.2) A Microprocessor Based System (MBS). Capabilities: generation of session key, comparison of two keys, lock door, unlock door.
(2.3) Small Persistent Memory (SPM).
(2.4) Electronically Controlled Door (ECD).

Operation of Solution 2

In this section we will describe the operation of the Solution 2 using pseudocode.

High-level operation of the system during start stage.
User selects an unused instrumented machine.
User loads the machine with his/her clothing for normal operation.
User inserts SC into the instrumented machine CAD.
The MBS computes a session key (SKIM).
The MBS stores the SKIM in its persistent memory.
The MBS stores a copy of the session key SKSC in the smart card persistent memory.
(Note that the value of SKIM is identical to SKSC, but they are stored in different places.)
The MBS locks the door of the instrumented machine.
The user pushes proper start buttons of the instrumented machine.
The instrumented machine starts its normal operation.
(At this point, the user is free to leave the instrumented machine, since the door is safely locked.)

High-level operation of the system during stop stage.
The user returns to the instrumented machine.
The user inserts the smart card into the instrumented machine CAD.
The MBS reads the session key SKSC from the smart card.
The MBS reads its session key SKIM from its persistent memory.
The MBS compares the SKSC and SKIM for equality.
If the compare operation results in an equality, the MBS issues command to unlock the door.
The user removes the smart card from the CAD.
The user removes his/her possessions from the instrumented machine.
If the compare results in inequality, the door will remain locked.

SOLUTION 3

In this section we will describe the subsystems comprising the Solution 3.

Systems comprising Solution 3:

The total system consists of two subsystems.

(1) Microprocessor Smart Card (CSC) (carried by the user), contains microprocessor and persistent memory. Capabilities: generation of session key, comparison of two keys.
(2) System attached to the instrumented machine (for example a washer or dryer).

The instrumented machine system consists of the following subsystems.
(2.1) Card Acceptance Device (CAD).
(2.2) A Logical Decision Circuit (LDC). Capabilities: lock door, unlock door.
(2.3) Small Persistent Memory (SPM).
(2.4) Electronically Controlled Door (ECD).

Operation of Solution 3

In this section we will describe the operation of the Solution 3 using pseudocode.

High-level operation of the system during start stage.

```
User selects an unused instrumented machine.
User loads the machine with his/her clothing for normal operation.
User inserts CSC into the instrumented machine CAD.
The CSC computes a session key (SKSC).
The CSC stores the SKSC in its persistent memory.
The LDC stores a copy of the session key SKIM in the instrumented machine persistent memory.
(Note that the value of SKIM is identical to SKSC, but they are stored in different places.)
The CSC returns a code to the LDC to lock the door of the instrumented machine.
The user pushes proper start buttons of the instrumented machine.
The instrumented machine starts its normal operation.
(At this point, the user is free to leave the instrumented machine, since the door is safely locked.)
```

High-level operation of the system during stop stage.

```
The user returns to the instrumented machine.
The user inserts the CSC into the instrumented machine CAD.
The CSC reads the session key SKIM from the instrumented machine.
The CSC reads its session key SKSC from its persistent memory.
The CSC compares  the SKSC and SKIM for equality.
If the compare operation results in equality, the CSC returns a code to the LDC to unlock the door.
The user removes the smart card from the CAD.
The user removes his/her possessions from the instrumented machine.
If the compare results in inequality, the door will remain locked.
```